MOBILE COMMUNICATION NETWORK, TERMINAL, PACKET COMMUNICATIO CONTROL METHOD, AND GATEWAY UNIT

Patent number: JP2001326697
Publication date: 2001-11-22
Inventor: TAKEDA SACHIKO; INAI HIDENORI; OISHI TAKUMI; SHIBATA JIRO
Applicant: HITACHI LTD
Classification:
- International: H04L12/66; H04L12/28; H04L12/56; H04L29/02
- european:
Application number: JP20000149808 20000517
Priority number(s):

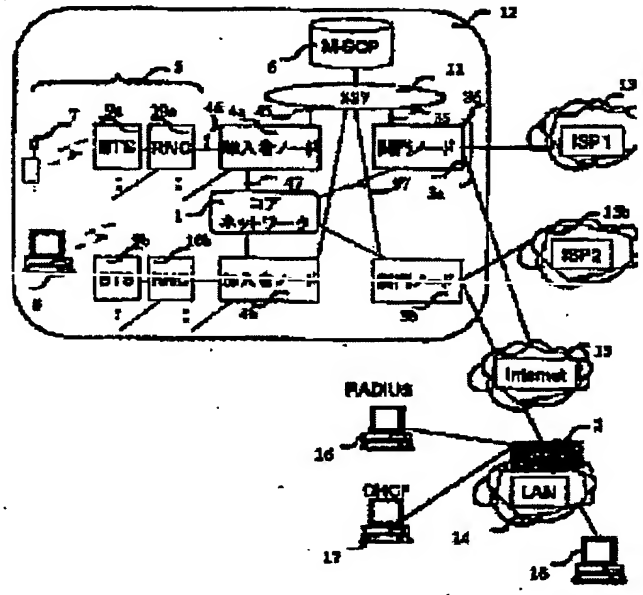
Also published as:
EP1156626 (A2)
US2001048686 (A
JP2001326697 (A)

Abstract of **JP2001326697**

PROBLEM TO BE SOLVED: To provide a mobile VPN service without having to use a mobile tunnel in an IPv6 mobile packet communication network.

SOLUTION: A mobile terminal transmits a control signal to enable packet transmission reception to a gateway node 3. The gateway node 3 discriminates presence or absence of a mobile VPN service request from connection destination information included in the signal. The gateway node 3 detecting the mobile VPN service request informs the mobile terminal about an IP address of the gateway node 3 via a subscriber node 4. The mobile terminal sets an IPv6 header 210 and an IPv6 path control header 220, so that the gateway node 3 relays the transmission packet without fail.

図1



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2001－326697
（Ｐ２００１－３２６６９７Ａ）
(43)公開日　平成13年11月22日(2001.11.22)

(51)Int.Cl.[7]	識別記号	ＦＩ			テーマコード（参考）
H04L 12/66		H04L 11/20		B	5K030
12/28		11/00	310	B	5K033
12/56		11/20	102	A	5K034
29/02		13/00	301	B	

審査請求　未請求　請求項の数15　ＯＬ　（全15頁）

(21)出願番号　特願2000－149808(Ｐ2000－149808)

(22)出願日　平成12年５月17日(2000.5.17)

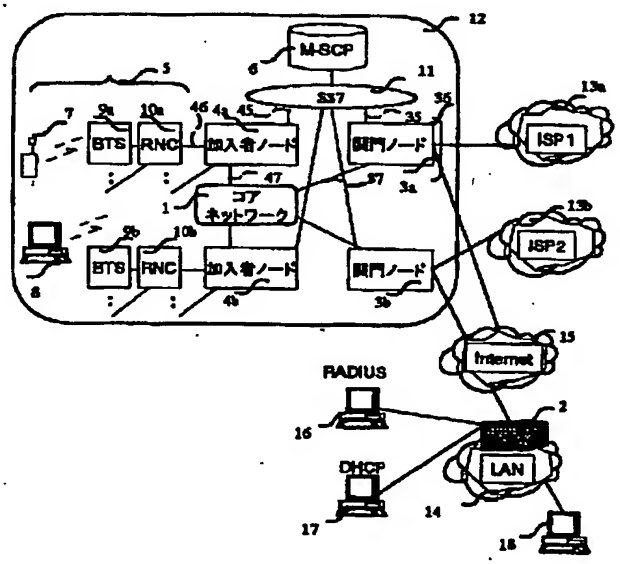
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　武田　幸子
東京都国分寺市東恋ケ窪一丁目280番地
株式会社日立製作所中央研究所内
(72)発明者　井内　秀則
東京都国分寺市東恋ケ窪一丁目280番地
株式会社日立製作所中央研究所内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】移動体通信網、端末装置、パケット通信制御方法、及び、関門装置

(57)【要約】
【課題】ＩＰｖ６移動体パケット通信網において、モバイルトンネルを利用することなくモバイルＶＰＮサービスを提供する。
【解決手段】移動端末は、関門ノード３にパケット送受信を可能にするための制御信号を送信する。関門ノード３は、上記信号に含まれる接続先情報から、モバイルＶＰＮサービス要求の有無を判別する。モバイルＶＰＮサービス要求を検出した関門ノード３は加入者ノード４経由で移動端末に上記関門ノード３のＩＰアドレスを通知する。移動端末は、送信パケットが必ず上記関門ノード３を中継するようにＩＰｖ６ヘッダ２１０とＩＰｖ６経路制御ヘッダ２２０を設定する。
【効果】ＩＰｖ６機能を活用することより、移動体パケット通信網において、モバイルトンネルを利用することなくモバイルＶＰＮサービスの提供が可能になる。

図1



【特許請求の範囲】

【請求項１】加入者装置と、該加入者装置との通信手段を有する複数の関門装置とを有し、
上記加入者装置は、端末装置からの通信要求を受け取ると、上記通信要求に対応する関門装置を選択し、
上記選択された関門装置は、上記通信要求に対応する通信網または通信網上の装置を特定するとともに、上記選択された関門装置のアドレス情報を上記端末装置に通知することを特徴とする移動体通信網。

【請求項２】上記端末装置の加入者情報を記憶したサービス制御装置をさらに有し、
上記関門装置は、上記加入者情報から上記通信要求に対応する通信網または通信網上の装置を特定する請求項１記載の移動体通信網。

【請求項３】上記選択された関門装置は上記通信要求において特定サービスが指定されていない場合には、上記選択された関門装置のアドレス情報を上記端末装置に通知しない請求項１記載の移動体通信網。

【請求項４】移動体通信網の加入者装置にAPNを含む通信要求を行い、
上記APNにより特定される関門装置から該関門装置のアドレス情報を受取り、該アドレス情報を利用してパケットのIPv6ヘッダ及びIPv6経路制御ヘッダを組み立てて、該パケットを送信する端末装置。

【請求項５】接続先となる通信網または通信網上の装置を特定する情報を上記通信要求に含める請求項４に記載の端末装置。

【請求項６】上記移動体通信網に特定サービスを要求しない場合には、通常のＩＰｖ６パケットを送信する請求項４記載の端末装置。

【請求項７】端末装置と、加入者装置と、加入者装置や他の通信網との通信手段を有する関門装置とからなるパケット通信網において、
上記加入者装置と上記関門装置は、加入者毎の位置情報やサービス情報を備えるサービス制御装置との通信手段を備え、
上記関門装置は、他の通信網を介して企業網内の装置と通信する手段を備え、
上記端末装置は、上記パケット通信網上或いは他の通信網上の装置と情報の送受信を可能にするため、上記加入者装置経由で関門装置に制御信号を送信し、
上記関門装置は、加入者装置から送信された制御信号に含まれる接続先情報から、企業網内装置との通信要求を検出する第１の手段を備え、
上記関門装置が企業網内装置との通信要求を検出した時、上記関門装置のアドレス情報を含む制御信号を上記加入者装置に送信し、
上記加入者装置が、上記関門装置のアドレス情報を含む制御信号を上記端末装置に送信する第２の手段を備え、
上記端末装置が、受信信号に上記関門装置のアドレス情報が含まれる時、上記関門装置のアドレス情報をＩＰｖ６ヘッダ情報作成時に適用し、上記端末装置が送信するパケットが、上記特定関門装置を必ず中継するように、ＩＰｖ６パケットを組み立てる第３の手段を備えることにより、
上記端末装置が上記企業網内の装置宛に送信するパケットが、必ず上記特定関門装置を経由することを特徴とするパケット通信制御方法。

【請求項８】上記端末装置が、上記加入者装置から関門装置のアドレス情報を含む制御信号を受信した時、上記関門装置のアドレス情報を利用して、ＩＰｖ６ヘッダとＩＰｖ６経路制御ヘッダを作成し、
上記端末装置が送信するパケットが、上記特定関門装置を必ず中継するように、パケットを組み立てる手段を備えることにより、
上記端末装置が上記企業網内の装置宛に送信するパケットが、必ず上記特定関門装置を経由することを特徴とする請求項７に記載のパケット通信制御方法。

【請求項９】上記関門装置が接続先の特定に利用する情報は、
上記加入者装置が上記サービス制御装置に記憶されている上記端末装置の加入者情報から上記端末装置の接続先情報を読み出して、関門装置宛の制御信号に設定した接続先情報、或いは、端末装置がユーザによって上記端末装置に入力された接続先情報を加入者装置宛の制御信号に設定し、上記制御信号を受信した加入者装置が関門装置宛の制御信号に設定した接続先情報であることを特徴とする請求項７に記載のパケット通信制御方法。

【請求項１０】下線部分について明細書の記載がないと思われる端末装置と、加入者装置と、加入者装置や他の通信網との通信手段を有する関門装置とからなるパケット通信網において、
上記加入者装置と上記関門装置は、加入者毎の位置情報やサービス情報を備えるサービス制御装置との通信手段を備え、
上記関門装置は、他の通信網を介して企業網内の装置と通信する手段を備え、
上記端末装置は、上記パケット通信網上或いは他の通信網上の装置と情報の送受信を可能にするため、上記加入者装置経由で上記関門装置に制御信号を送信し、　上記関門装置が上記加入者装置から受信した制御信号には、ユーザが設定した接続先情報、或いは、サービス制御装置から読み出された接続先情報が必ず含まれ、
上記関門装置は、加入者装置から送信された制御信号に含まれる接続先情報から、企業網内装置との通信要求の有無を検出する第１の手段を備え、
第１の手段によって、上記関門装置が企業網内装置との通信要求を検出した時、上記関門装置が、上記関門装置のアドレス情報を含む制御信号を上記加入者装置に送信し、

上記加入者装置が、上記関門装置のアドレス情報を含む制御信号を上記端末装置に送信する第２の手段を備え、
上記端末装置が受信した信号に上記関門装置のアドレス情報が含まれる時、上記端末装置は上記関門装置のアドレス情報を利用して、ＩＰｖ６ヘッダとＩＰｖ６経路制御ヘッダを作成し、
上記端末装置が送信するパケットが、上記特定関門装置を必ず中継するように、パケットを組み立てる第３の手段を備え、
第１の手段によって、上記関門装置が企業網内装置との通信要求を検出しなかった時、上記関門装置は上記関門装置自身のアドレス情報を含まない制御信号を上記加入者装置に送信し、
上記加入者装置が、上記端末装置に上記関門装置のアドレス情報を含まない制御信号を送信し、
上記端末装置は、受信信号に上記関門装置のアドレス情報が含まれない時、通常のＩＰｖ６パケットを接続先に送信する手段を備え、
上記端末装置が、企業網内の装置宛にパケットを送信する場合には、上記端末装置が送信するパケットは、必ず上記特定関門装置を経由し、
上記端末装置が、通常のＩＰｖ６パケットを接続先に送信する場合には、上記ＩＰｖ６パケットは、各装置が保持する経路表に基づき、接続先に対して最適ルーティングされることを特徴とするパケット通信制御方法。
【請求項１１】パケット通信網に接続されており、加入者装置や、他のパケット通信網上の装置や他網の装置との通信手段と、加入者毎の位置情報やサービス情報を備えるサービス制御装置との通信手段を備える関門装置において、
他の通信網を介して企業網内の装置と通信する手段を備え、
加入者装置から移動端末のパケット送受信を可能にするための制御信号を受信し、上記制御信号に含まれる接続先情報から、企業網内の装置との通信が要求されていることを検出する第１手段を備えることを特徴とする関門装置。
【請求項１２】上記関門装置が、上記第１の手段により、企業網内の装置との通信要求を検出すると、上記企業網内の装置と通信を行うため、上記関門装置と企業網内と他の通信網とを接続する装置との間に上記移動端末用のコネクションを設定する機能を備えることを特徴とする請求項１１に記載の関門装置。
【請求項１３】上記関門装置が、上記第１の手段により、企業網内の装置との通信要求を検出すると、上記加入者装置に、上記関門装置自身の識別情報を含む制御信号を送信することを特徴とする請求項１１に記載の関門装置。
【請求項１４】パケット通信網に接続されており、端末装置や他の通信網との通信手段を有する関門装置やパケット通信網内の他の装置と通信を行う手段と、加入者毎の位置情報やサービス情報を備えるサービス制御装置と通信を行う手段を有する加入者装置において、
上記関門装置が他の通信網を介して企業網内の装置と通信する手段を有し、
上記端末装置が上記パケット通信網上或いは他の通信網上の装置と情報の送受信を開始する前に、上記関門装置に、予め定められた手順に従ってパケットの送受信を可能にするための制御信号を送信すると、上記関門装置は受信した制御信号から企業網内の装置との通信要求を検出し、
上記関門装置から上記関門装置自身の識別情報を含む制御信号を受信した場合に、上記端末装置宛に上記関門装置の識別情報を含む制御信号を送信する第２の手段を有することを特徴とする加入者装置。
【請求項１５】加入者装置と通信を行う手段を有する端末装置において、
上記加入者装置は、パケット通信網に接続されており、パケット通信網上の関門装置と通信を行う手段と、加入者毎の位置情報やサービス情報を備えるサービス制御装置と通信を行う手段を有し、
上記端末装置が上記パケット通信網上或いは他の通信網上の装置と情報の送受信を開始する前に、上記関門装置に、予め定められた手順に従ってパケットの送受信を可能にするための制御信号を送信すると、
上記関門装置は受信した制御信号から企業網内の装置との通信要求を検出し、
上記関門装置が、上記加入者装置に、上記関門装置自身の識別情報を含む制御信号を送信し、
上記端末装置が、上記制御信号を受信した上記加入者装置から上記関門装置の識別情報を含む制御信号を受信した場合、
上記端末装置が、上記関門装置の識別情報を利用して、送信パケットが、上記関門装置を中継するようにパケットを組み立てる第３の手段を有することを特徴とする端末装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】ＩＰｖ６移動体パケット通信網におけるパケット転送方法に関する。特にＩＰv6移動体パケット通信網とIPベース網の連携システムにおけるモバイルＶＰＮサービス提供方法に関する。
【０００２】
【従来の技術】インターネット及び移動通信サービスは、急速に普及している。
【０００３】インターネットにおける通信は、事実上の標準であるＩＰ（ＩｎｔｅｒｎｅｔＰｒｏｔｏｃｏｌ、ＲＦＣ７９１）プロトコルを用いるＩＰパケットの送信により行う。インターネットに接続される装置には、各装置を識別するため、世界で一意にＩＰアドレスが割り

当てられる。IPパケットのルーティングは、ＩＰアドレスを使って行う。

【０００４】ＩＰパケットを受信した装置は、ＩＰパケットのヘッダに含まれる着信先ＩＰアドレスを調べる。装置自身に着信先ＩＰアドレスを有する端末が存在しない場合、各装置は、ルーティングテーブルを利用して、ＩＰパケットを隣接ノードに転送する。ルーティングテーブルとは、IPアドレスと隣接ノードの対応表である。

【０００５】現在利用しているＩＰｖ４アドレスは、インターネットの普及に伴い枯渇する恐れがある。そこで、新しいアドレス体系であるＩＰｖ６アドレスの検討が行われている（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ、Ｖｉｒｓｉｏｎ　６　（ＩＰｖ６）　Ｓｐｅｃｉｆｉｃａｔｉｏｎ、ＲＦＣ　２４６０）。

【０００６】ＩＰｖ６は、拡張ヘッダの中で様々な機能を規定できる。ＩＰｖ６拡張ヘッダは、ＩＰｖ６ヘッダとペイロードの間に挿入される。経路制御ヘッダは、ＩＰｖ６拡張ヘッダの１つである。経路制御ヘッダを利用すれば、パケット送信者は、パケットが通過するべき中間ノードを指定できる。

【０００７】インターネットを利用するサービスとして、ＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）が注目されている。ＶＰＮサービスには、ＬＡＮ間接続ＶＰＮサービスとリモート・アクセスＶＰＮサービスがある。ＬＡＮ間接続ＶＰＮサービスは、ＬＡＮ間接続にインターネットを利用するサービスである。リモート・アクセスＶＰＮサービスは、外出中のユーザに企業内の装置へのアクセスを提供するサービスである。リモート・アクセスＶＰＮサービスは、ＶＰＮへのアクセス機能を持つ装置と企業内のＶＰＮ装置との間の通信にインターネットを利用する。外出中のユーザは、ダイアルアップ接続等でＶＰＮアクセス機能を持つ装置に接続する。

【０００８】ＶＰＮアクセス機能を備える装置とＶＰＮ装置の間の通信は、セキュリティを確保するため、トンネルを利用する。ＶＰＮアクセス機能を備える装置は、ユーザからＩＰパケットすると、受信パケットにＶＰＮ装置宛のヘッダを付加し（カプセル化）、ＶＰＮ装置に送信する。ＶＰＮ装置は、先に付加されたヘッダをとり（デカプセル化）、元のＩＰパケットを復元する。ＶＰＮ装置は、元のＩＰパケットヘッダの宛先アドレスに書かれている装置宛にＩＰパケットを送信する。ＶＰＮに利用するトンネルをＶＰＮトンネルと呼ぶ。ＶＰＮトンネルには、例えば、Ｌ２ＴＰ（Ｌａｙｅｒ　Ｔｗｏ　Ｔｕｎｎｅｌｉｎｇ　Ｐｒｏｔｏｃｏｌ、ＲＦＣ　２６６１）がある。

【０００９】近年の移動通信サービスでは、データ通信の割合が増加している。移動通信網において、データ通信を効率的に提供するため、移動体パケット通信網の検討が活発化している。移動体パケット通信網の例として、ＰＤＣ－Ｐ（ＰＤＣ-Ｐａｃｋｅｔ）やＧＰＲＳ（Ｇｅｎｅｒａｌ　Ｐａｃｋｅｔ　Ｒａｄｉｏ　Ｓｅｒｖｉｃｅ）がある。第3世代移動体通信システムＩＭＴ－２０００においても高速パケット通信サービスの提供が予定されている。現在、移動体パケット通信網の上位通信プロトコルとして、ＩＰ(Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ)が普及している。

【００１０】移動体パケット通信網において、ＩＰプロトコルによる通信サービスを提供するため、通信事業者は移動端末にＩＰアドレスを割り当てる必要がある。移動端末の急増とＩＰｖ４アドレスの枯渇に伴い、移動端末にＩＰｖ６アドレスを割り振りることが予想される。

【００１１】一般に移動体通信網は、無線アクセス網とコア網からなる。無線アクセス網は、基地局や基地局制御装置から構成される。コア網は、加入者ノードや関門ノードから構成される。

【００１２】移動体通信網における通信形態は、移動端末発固定端末着、固定端末発移動端末着、移動端末発移動端末着の３種類に分類される。

【００１３】以下、例として、ＧＰＲＳ方式ベース移動端末発移動端末着のパケット通信手順を説明する。

【００１４】ＧＰＲＳ方式ベース移動体パケット通信網の移動端末は、まず、端末自身の位置情報を移動体パケット通信網に登録する。次に、ＧＰＲＳ独自の信号手順を利用して、発信端末がパケットの送受信を行えるようにするため、発信端末と関門ノードの間で制御信号を送信する。その後、移動端末は、着側移動端末に、ＩＰパケットを送信する。

【００１５】移動端末が着側移動端末宛に送信したＩＰパケットは、移動端末が在圏する加入者ノードを通過する。上記加入者ノードは、受信ＩＰパケットに、発側の本拠地（ホーム）関門ノード宛のヘッダを付加し（カプセル化）、発側ホーム関門ノードにパケットを送信する。発側ホーム関門ノードは、先に付加されたヘッダをとり（デカプセル化）、元のＩＰパケットを復元する。発側ホーム関門ノードは、元のＩＰパケットヘッダの宛先アドレスに含まれる着側移動端末のＩＰアドレスから、着側移動端末のホーム関門ノードを特定し、ＩＰパケットを転送する。着側ホーム関門ノードは、ＩＰパケットヘッダの宛先アドレスから、着側移動端末が在圏する加入者ノードを特定する。着側ホーム関門ノードは、再びＩＰパケットをカプセル化して、着側移動端末の在圏加入者ノードに向けてＩＰパケットを送信する。在圏加入者ノードは、受信パケットをデカプセル化して元のＩＰパケットを復元した後、着側移動端末にＩＰパケットを転送する。以上の処理により、発側移動端末が送信したＩＰパケットは、着側移動端末に到着する。

【００１６】ＩＰパケットをカプセル化した後、デカプセル化されて元のＩＰパケットを復元するまでの区間は、トンネルと呼ばれる。移動通信に利用するトンネル

をモバイルトンネルと呼ぶ。モバイルトンネルは、移動ユーザを追跡するために必要である。

【００１７】一方、ＩＥＴＦは、ＩＰｖ６アドレス対応のＭｏｂｉｌｅ　ＩＰ仕様を検討中である。Ｍｏｂｉｌｅ　ＩＰ　ｖ６の発信端末は、プロバイダが着移動端末に割り当てたｈｏｍｅ　ａｄｄｒｅｓｓ宛にパケットを送信する。着移動端末のＨｏｍｅ　Ａｇｅｎｔは、上記ｈｏｍｅ　ａｄｄｒｅｓｓ宛パケットを受信する。上記Ｈｏｍｅ　Ａｇｅｎｔは、受信パケットに着移動端末の在圏アドレスを含むヘッダを付加し、着移動端末に転送する。在圏アドレスとは、移動端末の在圏網が移動端末に動的に割り当てるＩＰアドレスである。

【００１８】パケットを受信した着移動端末は、発信端末に着移動端末自身の在圏アドレスを含む制御信号を送信する。上記発信端末は、上記制御信号に含まれる着移動端末の在圏アドレス情報を記憶する。上記発信端末が着移動端末の在圏アドレス情報を保持する場合、発信端末は着移動端末にパケットを送信する時、着移動端末の在圏アドレスを利用できる。

【００１９】モバイルＶＰＮサービスは、第3世代移動体通信システム（ＩＭＴ－２０００）の主要サービスになると予想されている。モバイルＶＰＮサービスは、リモート・アクセスＶＰＮの１形態であり、外出中のユーザが移動体パケット通信網を利用して、企業内の装置にアクセスするサービスである。モバイルＶＰＮサービスは、移動端末発固定端末着の通信である。

【００２０】モバイルＶＰＮサービスを提供するため、特願２０００－９７８１３に記載されているように、移動体パケット通信網の関門ノードは、ＶＰＮアクセスサーバ機能を備える。モバイルＶＰＮサービスでは、関門ノードとＶＰＮ装置の間の通信に、ＶＰＮトンネルを利用する。このため、移動端末が送信するパケットは、通信開始時にアクセスしたＶＰＮアクセスサーバ機能付き関門ノードを必ず経由する必要がある。

【００２１】

【発明が解決しようとする課題】現在の移動体パケット通信網は、加入者ノードと関門ノードの間の通信にモバイルトンネルを利用する。加入者ノードと関門ノードが、パケットのカプセル化・デカプセル化処理を行う。この時、パケットのカプセル化・デカプセル化に伴う加入者ノードと関門ノードの処理が増加し、移動体パケット通信網のスループットが低下するという課題がある。

【００２２】しかし、モバイルトンネルを利用しない場合、移動端末が送信するＩＰパケットは、ＩＰヘッダに基づいてルーティングされる。このため、上記パケットが、該当端末用のＶＰＮトンネルが設定されている関門ノードを必ず経由するとは限らない。パケットが上記関門ノードを通過しない場合、ユーザが、モバイルＶＰＮサービスを利用できないという課題がある。

【００２３】

【課題を解決するための手段】上記課題を解決するため、本発明によるＩＰｖ６移動体パケット通信網におけるパケット通信制御方法では、ＩＰｖ６経路制御ヘッダを利用してパケットを転送する。関門ノードは、移動体パケット通信網で利用されている制御信号を活用して、移動端末に経路制御ヘッダの作成に必要な情報を送信する。

【００２４】移動端末は、まず、端末自身の位置情報を移動体パケット通信網に登録する。次に、発信端末は、データパケットの送受信を可能にするため、加入者ノードに制御メッセージ（Ａｃｔｉｖａｔｅ　ＰＤＰ　Ｃｏｎｔｅｘｔ　Ｒｅｑｕｅｓｔ）を送信する。上記制御メッセージを受信した加入者ノードは、ＡＰＮ（Ａｃｃｅｓｓ　Ｐｏｉｎｔ　Ｎａｍｅ）から関門ノードを特定する。加入者ノードは、次のいずれかの手段により、ＡＰＮを取得する。移動端末の接続先が固定されている場合、ＡＰＮは移動用サービス制御装置（Ｍ－ＳＣＰ）に格納されており、移動端末の位置登録時に、加入者ノードがＭ－ＳＣＰから読み出す。移動端末の接続先が可変である場合、移動端末ユーザが入力したＡＰＮが、Ａｃｔｉｃａｔｅ　ＰＤＰ　Ｃｏｎｔｅｘｔ　ＲｅｑｅｕｓｔのＡＰＮパラメータに設定される。

【００２５】加入者ノードは、特定した関門ノードに、移動端末がデータパケットの送受信をできるようにするため、制御メッセージ（Ｃｒｅａｔｅ　ＰＤＰ　Ｃｏｎｔｅｘｔ　Ｒｅｑｕｅｓｔ）を送信する。上記メッセージには、ＡＰＮパラメータが必ず含まれる。上記メッセージを受信した関門ノードは、受信メッセージ中のＡＰＮパラメータから接続先の外部ネットワークを特定する。

【００２６】ここで、関門ノードは、ＡＰＮからモバイルＶＰＮサービスの要求を検出する第1の手段を備える。モバイルＶＰＮサービスを利用する場合、関門ノードは、関門ノード自身のＩＰアドレスを含む応答メッセージ（Ｃｒｅａｔｅ　ＰＤＰＣｏｎｔｅｘｔ　Ｒｅｓｐｏｎｓｅ）を加入者ノードに送信する。

【００２７】上記加入者ノードは、上記関門ノードのＩＰアドレスを含むＣｒｅａｔｅ　ＰＤＰ　Ｃｏｎｔｅｘｔ　Ｒｅｓｐｏｎｓｅを受信した時、上記関門ノードのＩＰアドレスを含むＡｃｔｉｖａｔｅ　ＰＤＰ　Ｃｏｎｔｅｘｔ　Ａｃｃｅｓｐｔメッセージを移動端末に送信する第２の手段を備える。

【００２８】上記加入者ノードが関門ノードから上記関門ノードのＩＰアドレスを含まない応答メッセージを受信した時、加入者ノードは移動端末に上記関門ノードのＩＰアドレスは通知しない。

【００２９】移動端末は、加入者ノードから関門ノードのＩＰアドレスを含む応答メッセージを受信すると、パケット送信時に必ずＩＰｖ６経路制御ヘッダを利用する第３の機能を備える。移動端末は、送信パケットが、必

ず該当端末のＶＰＮトンネルが設定さている上記関門ノードを通過するように、ＩＰｖ６ヘッダとＩＰｖ６経路制御ヘッダを組み立てる。ＩＰｖ６経路制御ヘッダを利用すれば、パケット送信者は、パケットが通過するべき中間ノードとして、上記関門ノードを指定できる。

【００３０】移動端末が、上記加入者ノードから関門ノードのＩＰアドレスを含まない応答メッセージを受信した場合、移動端末は、パケット送信時にＩＰｖ６経路制御ヘッダは利用しない。

【００３１】即ち、移動端末は、送信パケットの中継経路を指定しない。この場合、移動端末が送信するパケットは、各ノードが保持するルーティングテーブル情報に基づき転送される。従って、移動端末が送信するパケットは、特定の関門ノードを中継するとは限らない。移動端末がモバイルＶＰＮサービスを利用しない場合は、移動端末が送信するパケットは特定関門ノードを通過する必要はないため、問題はない。

【００３２】ＩＰｖ６経路制御ヘッダを含むＩＰパケットを受信した関門ノードは、まず、ＩＰｖ６経路制御ヘッダを処理する。次に、受信パケットにＶＰＮトンネル用の付加ヘッダを追加し、ＶＰＮ装置宛に送信する。

【００３３】移動端末がＩＰｖ６経路制御ヘッダを使ってパケットを送信すれば、上記移動端末は送信パケットの中継ノードに、該当端末のＶＰＮトンネルが設定されている特定関門ノードを指定できる。従って、モバイルトンネルを利用することなく、移動端末ユーザにモバイルＶＰＮサービスを提供できる。

【００３４】本発明によれば、移動体パケット通信網が上記１から上記３の手段を備えることにより、モバイルトンネルを利用せずに、移動端末ユーザにモバイルＶＰＮサービスを提供できる。

【００３５】移動体パケット通信網において、ＩＰｖ６機能を活用することにより、ネットワーク提供者は、通信サービスを効率的に提供できる。

【００３６】

【発明の実施の形態】本発明の第１の実施の形態を図面を用いて説明する。

【００３７】図１は、本発明によるモバイルＶＰＮサービスをサポートするネットワークの構成例を示す。

【００３８】モバイルＶＰＮサービスをサポートするネットワークは、移動体パケット通信網１２とインターネット１５とＬＡＮ１４から構成される。本発明では、移動体パケット通信網１２とＬＡＮ１４は、ＩＰｖ６アドレスを利用する。

【００３９】移動体パケット通信網１２は、無線アクセス網５とコア網１から構成される。

【００４０】移動体パケット通信網１２のコア網１は、複数の加入者ノード４と、複数の関門ノード３から構成される。加入者ノード４、及び、関門ノード３は、共通線信号網１１を介してＭ－ＳＣＰ６に接続される。

【００４１】関門ノード３は、ＩＳＰ１３、或いは、Ｉｎｔｅｒｎｅｔ１５など、移動体パケット通信網１２以外の網とインターネットプロトコルによって通信する手段を持つ。また、関門ノード３ｂは、ＶＰＮアクセスサーバ機能を備え、ＬＡＮ１４のＶＰＮ装置２にアクセスできる。

【００４２】移動体パケット通信網１２の無線アクセス網５は、複数の基地局（ＢＴＳ）９（９ａ、９ｂ）と、複数の基地局制御装置（ＲＮＣ）１０（１０ａ、１０ｂ）によって構成される。

【００４３】Ｍ－ＳＣＰ６は、加入者情報と、端末の位置情報と、加入者に提供する付加サービスのプログラムを備える。

【００４４】ＬＡＮ１４には、ＶＰＮ装置２と、各種情報を提供するサーバ１８が接続される。ＬＡＮ１４に、ＶＰＮサービス加入者の認証情報を備えるＲＡＤＩＵＳ（Ｒｅｍｏｔｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｄｉａｌ ＩＮ Ｕｓｅｒ Ｓｅｒｖｉｃｅ）サーバ１６やＶＰＮサービスを利用する端末にＩＰアドレスを割り当てるＤＨＣＰ（Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）サーバ１７を接続してもよい。

【００４５】ＶＰＮ装置２は、Ｉｎｔｅｒｎｅｔ１５とインターネットプロトコルで通信する手段を持つ。

【００４６】図２は、関門ノード３の構成を示す。関門ノード３は、加入者ノード４や他網との間の信号を制御するＣＰＵ３１と、メモリ３２と、共通線信号網との間の信号線３５を終端する信号線終端部３３と、他のＩＰ網との間の信号線３６や、コア網１内の他のノードとの間の信号線３７を終端するＩＰ網インタフェース部３４（３４ａ、３４ｂ）をバス３８で接続する構成となっている。

【００４７】ＣＰＵ３１と加入者ノードや他網との間の通信は、例えば、インターネットプロトコルを用いて行われる。

【００４８】メモリ３２は、他のＩＰ網上の装置、或いは、コア網１上の装置と信号を送受信するプログラムや、移動端末がパケット通信に利用する制御情報を生成・修正・削除するプログラムや、ＬＡＮ１４のＶＰＮ装置２にアクセスするためのＶＰＮアクセスサーバ機能を実現するプログラムや、図３に示すモバイルＶＰＮサービスの検出を行うＶＰＮ判別処理ルーチン６０や、図４に示すユーザ情報管理テーブル３００を備える。

【００４９】スイッチ３９は、ＩＰ網インタフェース部３４が接続され、ノード３内におけるスイッチング機能を実現する。

【００５０】図４は、ユーザ情報管理テーブル３００のテーブル構成を示す。本テーブルは、移動体パケット通信網加入者識別子（ＩＭＳＩ）３０１毎に生成された複数のエントリ（３００－１～３００－ｎ）からなる。各

エントリは、ＩＭＳＩ３０１対応に、ＩＰアドレス３０２と、端末が在圏する加入者ノードのＩＰアドレス３０３と、モバイルＶＰＮサービスの利用を示すＶＰＮフラグ３０４と、関門ノードとＶＰＮ装置間に設定したＶＰＮトンネルを識別するＶＰＮトンネル識別子３０５とＶＰＮセッション識別子３０６を定義する。

【００５１】図７は、端末（７、８）と関門ノード３との間で送信されるＩＰｖ６パケットのフォーマットを示す。ＩＰパケット２００は、ＩＰｖ６ヘッダ２１０と、ＩＰｖ６拡張ヘッダ２２０と、ペイロード２３０とからなる。ＩＰｖ６では、ＩＰｖ６ヘッダの次に拡張ヘッダ２２０を挿入できる。本発明では、拡張ヘッダの１つである経路制御ヘッダ（Ｒｏｕｔｉｎｇ　Ｈｅａｄｅｒ）を利用する。従って、図７は、ＩＰｖ６拡張ヘッダ２２０に、経路制御ヘッダを用いた場合のパケットフォーマットを示している。

【００５２】ＩＰｖ６ヘッダ２１０は、バージョン番号、トラヒッククラス、フローラベル、ペイロード長、後続ヘッダタイプ２１１、ホップ・リミット、送信元アドレス２１２、宛先アドレス２１３から構成される。後続ヘッダタイプ２１１は、ＩＰｖ６ヘッダ２１０に後続するヘッダを識別する。ペイロード２３０に通常の上位プロトコル・データ単位（ＰＤＵ）が入る場合には、後続ヘッダタイプ２１１に、上位プロトコルのプロトコル番号が設定される。ＩＰｖ６拡張ヘッダ２２０がＩＰｖ６ヘッダに後続する場合は、後続ヘッダタイプ２１１にＩＰｖ６拡張ヘッダの種類を示す値が設定される。

【００５３】宛先アドレス２１３には、通常、最終目的地のＩＰｖ６アドレスを設定する。ただし、経路制御ヘッダを用いる場合は、宛先アドレス２１３に、最終宛先ではなく、パケットを次に中継するべきノードのアドレスを設定する。

【００５４】経路制御ヘッダは、後続ヘッダタイプ、ヘッダ長、ルーティング・タイプ、残余セグメント数２２１、アドレス２２２から構成される。残余セグメント数２２１には、未通過の中間ノード数を設定する。アドレス２２２には、パケットを中継するべき中間ノードのアドレスを設定する。アドレス２２２に、複数の中間ノードアドレスを設定してもよい。

【００５５】本発明において、モバイルＶＰＮサービスを利用する移動端末が送信するＩＰパケットは、ＩＰｖ６ヘッダ２１０の後続ヘッダタイプ２１１に経路制御ヘッダタイプを、送信元アドレス２１２に端末のＩＰアドレスを、宛先アドレス２１３に関門ノードのＩＰアドレスをそれぞれ設定する。経路制御ヘッダのアドレス２２２には、移動端末が指定した通信先ノード１８のＩＰアドレスを、残余セグメント数２２１には１をそれぞれ設定する。

【００５６】図８は、関門ノード３とＶＰＮ装置２との間で、Ｌ２ＴＰによるＶＰＮトンネルを利用してパケット転送を行う場合のパケットフォーマット２５０を示す。

【００５７】関門ノード３は、移動端末から受信したＩＰｖ６パケット２００にＶＰＮトンネル用のヘッダ２４０（ＩＰヘッダ２４１、ＵＤＰヘッダ２４２、Ｌ２ＴＰヘッダ２４３）を付加する。

【００５８】関門ノード３がＶＰＮ装置２にパケットを送信する時、ＶＰＮヘッダ２４０に設定する情報は、次の通りである。ＩＰヘッダ２４１の宛先アドレスにＶＰＮ装置２のＩＰアドレスを、送信元アドレスに関門ノード３のＩＰアドレスを設定する。ＵＤＰヘッダ２４２の宛先ポート番号に、データ送信先のアプリケーションが“Ｌ２ＴＰ”であることを示すポート番号「１７０１」を設定する。Ｌ２ＴＰヘッダ２４３には、ＶＰＮトンネルを識別するＩＤや、ＶＰＮトンネル内のセッションを識別するＩＤを設定する。

【００５９】図３は、モバイルＶＰＮサービスの検出を行うＶＰＮ判別処理ルーチン６０を示す。本ルーチンは、関門ノード３が、加入者ノード４から、Ｃｒｅａｔｅ　ＰＤＰ　Ｃｏｎｔｅｘｔ　Ｒｅｑｕｅｓｔメッセージを受信した場合に起動される。

【００６０】ＶＰＮ判別処理ルーチン６０は、上記受信メッセージに必ず含まれるＡＰＮを読み出し、モバイルＶＰＮサービス要求の有無を判別する（ステップ６１）。

【００６１】モバイルＶＰＮサービスが要求されている場合、関門ノード３は、ＶＰＮサービスへのアクセス可否を判断するため、例えば、ＬＡＮ上のＲＡＤＩＵＳサーバ１６にＶＰＮ認証要求を送信する（ステップ６２）。関門ノード３は、ＶＰＮ認証処理待ち状態になる（ステップ６３）。

【００６２】ＶＰＮ認証応答を受信した上記関門ノード３は、認証処理が正常終了したかを判別する（ステップ６４）。正常終了時、上記関門ノード３は、自身のＩＰアドレスを含む応答メッセージ（Ｃｒｅａｔｅ　ＰＤＰ　Ｃｏｎｔｅｘｔ　Ｒｅｓｐｏｎｓｅ）を加入者ノード４に送信し（ステップ６５）、本ルーチンを終了する。認証処理がエラー終了した時、上記関門ノード３は、エラー通知を含む応答を加入者ノード４に送信し（ステップ６７）、本ルーチンを終了する。

【００６３】ステップ６１において、モバイルＶＰＮサービス要求が検出されない場合、関門ノード３は、自身のＩＰアドレスを含まない応答を加入者ノード４に送信し（ステップ６６）、本ルーチンを終了する。

【００６４】上記加入者ノード４は、受信信号に関門ノード３のＩＰアドレスが含まれている時、移動端末に、上記関門ノード３のＩＰアドレスを含むＡｃｔｉｖａｔｅＰＤＰ　Ｃｏｎｔｅｘｔ　Ａｃｃｅｓｐｔメッセージを送信する。

【００６５】上記加入者ノード４は、受信信号に関門ノ

ード３のIPアドレスが含まれない時、移動端末に、上記関門ノード３のＩＰアドレスを含まないＡｃｔｉｖａｔｅＰＤＰ　Ｃｏｎｔｅｘｔ　Ａｃｃｅｓｐｔメッセージを送信する。

【００６６】上記加入者ノード４は、受信信号にエラー通知が含まれる時、移動端末に、Ａｃｔｉｖａｔｅ　ＰＤＰ　Ｃｏｎｔｅｘｔ　Ｒｅｊｅｃｔメッセージを送信する。

【００６７】次に、図５と図６に示す信号シーケンスに従って、図１に示したネットワークにおけるモバイルＶＰＮサービスを提供するための処理手順を説明する。

【００６８】図５は、移動体パケット通信網１２に加入している移動端末７のユーザが、モバイルＶＰＮサービスの利用を開始するために必要な処理手順を示す。

【００６９】本発明の実施の形態では、移動体パケット通信網における制御信号にＧＰＲＳベースの制御信号を用いて説明する。

【００７０】移動端末７は、まず、移動端末の位置情報を移動体パケット通信網に登録する。

【００７１】移動端末７は、移動体パケット通信網加入者識別子（ＩＭＳＩ）を含むＡｔｔａｃｈ　Ｒｅｑｅｕｓｔメッセージ１００を加入者ノード４ａに送信する。加入者ノード４ａは、受信メッセージ１００に含まれるＩＭＳＩに基づいて、加入者情報を保持するＭ－ＳＣＰ６を決定し、上記Ｍ－ＳＣＰ６に加入者情報読出要求メッセージ１０１を送信する。

【００７２】上記Ｍ－ＳＣＰ６は、受信メッセージ１０１に含まれるＩＭＳＩに基づき、該当ＩＭＳＩの認証情報を読み出し、上記認証情報を含む加入者情報読出応答メッセージ１０２を上記加入者ノード４ａに送信する。

【００７３】上記加入者ノード４ａは、移動端末７との間で認証処理を行う（１０３）。

【００７４】認証処理が正常終了した場合、上記加入者ノード４ａは、上記Ｍ－ＳＣＰ６に自身のＩＰアドレスを含むＵｐｄａｔｅ　Ｌｏｃａｔｉｏｎメッセージ１０４を送信する。

【００７５】上記メッセージ１０４を受信したＭ－ＳＣＰ６は、該当ＩＭＳＩの位置情報として、上記加入者ノード４ａのＩＰアドレスを記憶する。続いて、上記Ｍ－ＳＣＰ６は、加入者ノード４ａに加入者の契約情報等を含むＩｎｓｅｒｔ　Ｓｕｂｓｃｒｉｂｅｒ　Ｄａｔａメッセージ１０５を送信する。加入者ノード４ａは、受信情報を記憶した後、Ｍ―ＳＣＰ６にＩｎｓｅｒｔ　Ｓｕｂｓｃｒｉｂｅｒ　Ｄａｔａ　Ａｃｋメッセージ１０６を送信する。Ｍ－ＳＣＰ６は、上記加入者ノード４ａに、位置情報登録終了を示すＵｐｄａｔｅ　Ｌｏｃａｔｉｏｎ　Ａｃｋメッセージ１０７を送信する。上記メッセージ１０７を受信した加入者ノード４ａは、Ａｔｔａｃｈ　Ａｃｃｅｐｔメッセージ１０８を移動端末７に送信する。

【００７６】移動端末７の接続先が固定的に登録されている場合、ＡＰＮは、上記メッセージ１０５の契約情報に含まれる。

【００７７】次に、移動端末７は、パケットの送受信を可能にするための処理を行う。移動端末７は、ＩＭＳＩを含むＡｃｔｉｖａｔｅ　ＰＤＰ　Ｃｏｎｔｅｘｔ　Ｒｅｑｕｅｓｔメッセージ１０９を加入者ノード４ａに送信する。

【００７８】移動端末の接続先が可変である場合、移動端末ユーザが入力したＡＰＮが上記メッセージ１０９に含まれる。

【００７９】上記加入者ノード４ａはＡＰＮから関門ノードを特定し、関門ノード３ｂにＡＰＮを含むＣｒｅａｔｅ　ＰＤＰ　Ｃｏｎｔｅｘｔ　Ｒｅｑｕｅｓｔメッセージ１１０を送信する。受信メッセージ１１０に含まれるＡＰＮは、通信要求に対応する通信網、又は、通信網上の装置を特定するために利用する。

【００８０】上記関門ノード３ｂは、受信メッセージ１１０に含まれる加入者ノードＩＰアドレスをユーザ情報管理テーブル３００の該当ＩＳＭＩに対応する加入者ノードＩＰアドレス３０３に格納する。次に、上記関門ノード３ｂは、図３に示すＶＰＮ判別処理ルーチン６０を起動し、モバイルＶＰＮサービス要求の有無を判別する（１１１）。

【００８１】モバイルＶＰＮサービスが要求される場合、関門ノード３ｂは、図４に示すユーザ情報管理テーブル３００の該当ＩＭＳＩに対応するＶＰＮフラグ３０４を設定する。次に、ＶＰＮサービスへのアクセス可否を判断するため、関門ノード３ｂは、ＬＡＮ１４に接続されるＲＡＤＩＵＳサーバ１６に認証要求１１２を送信する。認証に成功した場合、上記ＲＡＤＩＵＳサーバ１６は、上記関門ノード３ｂに、認証成功を示す認証応答１１３を送信する。

【００８２】ここで、移動端末７にＩＰアドレスが割り振られていない場合、移動端末７にＩＰアドレスを割り振る手順を示す。ＩＰアドレスを割り振る手段として、例えば、ＩＰｖ６対応ＤＨＣＰを利用する。

【００８３】上記関門ノード３ｂは、ＬＡＮ１４にＩＰアドレス付与機能を持つＤＨＣＰサーバを検出するための制御信号（ＤＨＣＰ　Ｓｏｌｉｃｉｔ）１１４を送信する。上記信号１１４を受信したＤＨＣＰサーバ１７は、自身のアドレス情報を含む応答信号（ＤＨＣＰ　Ａｄｖｅｒｔｉｓｅ）１１５を上記関門ノード３ｂに送信する。次に上記関門ノード３ｂは、上記ＤＨＣＰサーバ１７にＩＰアドレス割り当て要求信号（ＤＨＣＰ　Ｒｅｑｅｕｓｔ）１１６を送信する。上記信号１１６を受信したＤＨＣＰサーバ１７は、移動端末７にＩＰアドレスを付与し（１１７）、上記関門ノード３ｂに上記ＩＰアドレスを含む応答信号１１８（ＤＨＣＰＲｅｐｌａｙ）を送信する。上記関門ノード３ｂは、割り当てられたＩ

Ｐアドレスを、図４に示すユーザ情報管理テーブル３００の該当ＩＭＳＩに対応するＩＰアドレス３０２に書きこむ。

【００８４】次に関門ノード３ｂは、関門ノード３ｂとＶＰＮ装置２の間にＶＰＮトンネルを設定する（１１９）。ＶＰＮトンネル設定後、加入者ノード３ｂは、該当ユーザのＶＰＮトンネルＩＤとセッションＩＤを図４に示すユーザ情報管理テーブル３００のＶＰＮトンネルＩＤフィールド３０５とＶＰＮセッションＩＤフィールド３０６に登録する。

【００８５】関門ノード３ｂは、割り当てられたＩＰアドレスと自身のＩＰアドレスを含むＣｒｅａｔｅ ＰＤＰ Ｃｏｎｔｅｘｔ Ｒｅｓｐｏｎｓｅを加入者ノード４ａに送信する（１２０）。上記加入者ノード４ａは、受信信号１２０に関門ノード３ｂのＩＰアドレスが含まれる場合、移動端末７に、上記関門ノード３ｂのＩＰアドレスと移動端末７に割り当てられたＩＰアドレスを含むＡｖｔｉｖａｔｅＰＤＰ Ｃｏｎｔｅｘｔ Ａｃｃｅｐｔを送信する（１２１）。

【００８６】上記移動端末７は、受信信号１２１に含まれる関門ノード３ｂのＩＰアドレスを記憶し、ＩＰｖ６パケット通信に利用する。

【００８７】ステップ１１１において、モバイルＶＰＮサービスの要求が検出されない場合の処理を以下に示す。関門ノード３ｂは、加入者ノード４ａに関門ノード３ｂ自身のＩＰアドレスを含まないＣｒｅａｔｅ ＰＤＰ Ｃｏｎｔｅｘｔ Ｒｅｓｐｏｎｓｅ１２０を送信する。上記加入者ノード４ａは、移動端末７に上記関門ノード３ｂのＩＰアドレスを含まないＡｃｔｉｖａｔｅ ＰＤＰ ＣｏｎｔｅｘｔＡｃｃｅｐｔ１２１を送信する。

【００８８】図６は、図５に示した処理を完了した移動端末７が、パケットデータの送信する時の処理手順を示す。特に、移動端末７は加入者ノード４ａから関門ノード３ｂのＩＰアドレス情報を受信した場合を示す。

【００８９】移動端末７は、図７に示したＩＰｖ６経路制御ヘッダを利用して、ＩＰｖ６パケットを送信する。移動端末７は、以下に示すようにＩＰｖ６パケット１３１の設定を行い、パケットを送信する。ＩＰｖ６ヘッダ２１０の宛先アドレス２１３に関門ノード３ｂのＩＰアドレスを設定する。ＩＰｖ６ヘッダ２１０の送信元アドレス２１２に移動端末７のＩＰアドレスを設定する。ＩＰｖ６ヘッダ２１０の後続ヘッダ２１１に経路制御ヘッダが続くことを示す値“４３”を設定する。ＩＰｖ６経路制御ヘッダ２２０のアドレス情報２２２にＬＡＮ１４内のサーバ１８のＩＰアドレスを設定する。残余セグメント数２２１に１を設定する。

【００９０】上記ＩＰｖ６パケット１３１を受信した関門ノード３ｂは、ＩＰｖ６経路制御ヘッダを処理する。具体的には、ＩＰｖ６ヘッダ２１０の宛先アドレス２１３にサーバ１８のＩＰアドレスを設定し、ＩＰｖ６経路制御ヘッダ２２０のアドレス情報２２２に関門ノード３ｂのＩＰアドレスを設定し、残余セグメント数２２１を１から０に変更する。

【００９１】上記関門ノード３ｂは、サーバ１８のＩＰアドレスのネットワークプレフィックスからモバイルＶＰＮサービスを利用中であることを判断し、ＶＰＮ装置２のＩＰアドレスを特定する。ＶＰＮ装置２のＩＰアドレスは、ＶＰＮヘッダ２４０内のＩＰヘッダ２４１の宛先アドレスに設定される。

【００９２】上記関門ノード３ｂは、受信パケット１３１のＩＰｖ６ヘッダ２１０内の送信元アドレス２１２を検索キーとして、ユーザ情報管理テーブル３００から該当移動端末７のＶＰＮトンネルＩＤ３０５とＶＰＮセッションＩＤ３０６を読み出す。上記ＶＰＮトンネルＩＤとＶＰＮセッションＩＤは、ＶＰＮヘッダ２４０内のＬ２ＴＰヘッダ２４３に設定される。

【００９３】関門ノード３ｂは、受信パケット１３１に、図８に示すＶＰＮヘッダ２４０を付加し、ＶＰＮ装置２宛にパケット１３２を送信する。

【００９４】上記ＶＰＮヘッダ２４０付きパケット１３２を受信したＶＰＮ装置２は、ＶＰＮヘッダ２４０を取り外し、元のＩＰパケットに含まれる宛先ＩＰアドレスが示すサーバ１８に、ＩＰパケット１３３を転送する。

【００９５】以上の処理を行うことにより、移動端末７がサーバ１８に送信するＩＰパケットは、必ず該当端末のＶＰＮトンネルが設定されている関門ノード３ｂを通過する。従って、ＩＰｖ６移動体パケット通信網において、モバイルトンネルを利用することなく、モバイルＶＰＮサービスを提供することが可能になる。

【００９６】次に、移動端末７が、加入者ノード４ａから関門ノード３ｂのＩＰアドレス情報を受信しなかった場合の処理手順を示す。

【００９７】移動端末７は、以下に示すようにＩＰｖ６パケット１３１の設定を行い、パケットを送信する。

【００９８】ＩＰｖ６ヘッダ２１０の宛先アドレス２１３にＬＡＮ１４内のサーバ１８のＩＰアドレスを設定する。ＩＰｖ６ヘッダ２１０の後続ヘッダ２１１に上位プロトコルのプロトコル番号（例：上位プロトコルがＴＣＰである場合には、“６”）を設定する。ＩＰｖ６パケット１３１は、ＩＰｖ６ヘッダ２１０とペイロード２３０とからなる。ＩＰｖ６パケット１３１は、経路制御ヘッダ２２０を含まない。従って、移動端末７は、送信パケットの中継経路を指定しないため、送信パケットが関門ノード３ｂを通過するとは限らない。移動端末がモバイルＶＰＮサービスを利用しない場合、移動端末７が送信するパケットは、各ノードのルーティングテーブルに情報に基づき転送される。

【００９９】

【発明の効果】以上の実施の形態の説明から明らかなよ

うに、本発明によれば、ＩＰｖ６移動体パケット通信網において、ＩＰｖ６の経路制御ヘッダを活用し、移動端末が送信するＩＰパケットが必ず特定の関門ノードを通過するように指定できる。従って、モバイルトンネルを利用することなく、モバイルＶＰＮサービスを提供することが可能になる。ＩＰｖ６の機能を活用して通信サービスを提供することにより、効率的な通信サービスの提供ができる。

【図面の簡単な説明】

【図１】移動体パケット通信網の構成の一例を示す図。

【図２】関門ノードの構成を示す図。

【図３】関門ノードで行うモバイルＶＰＮサービス要求を判別するフローチャート。

【図４】関門ノードが保持するユーザ情報管理テーブル構成を示す図。

【図５】本発明における、端末の発信処理手順を示す信号シーケンス。

【図６】本発明における、通信処理手順を示す信号シーケンス。

【図７】移動端末から関門ノードに送信されるＩＰｖ６パケットのフォーマット。

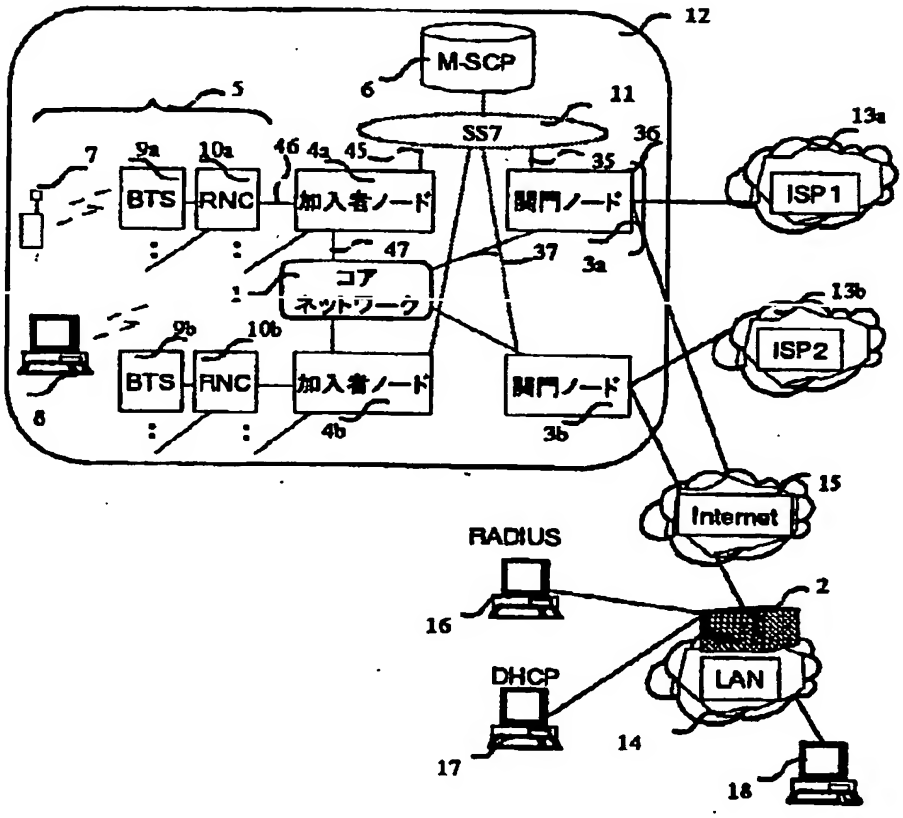
【図８】関門ノードからＶＰＮ装置に送信されるＩＰパケットのフォーマット。

【符号の説明】

２・・・ＶＰＮ装置、３・・・関門ノード、４・・・加入者ノード、６・・・移動サービス用サービス制御装置、７・・・移動端末、１４・・・ＬＡＮ、１８・・・サーバ。

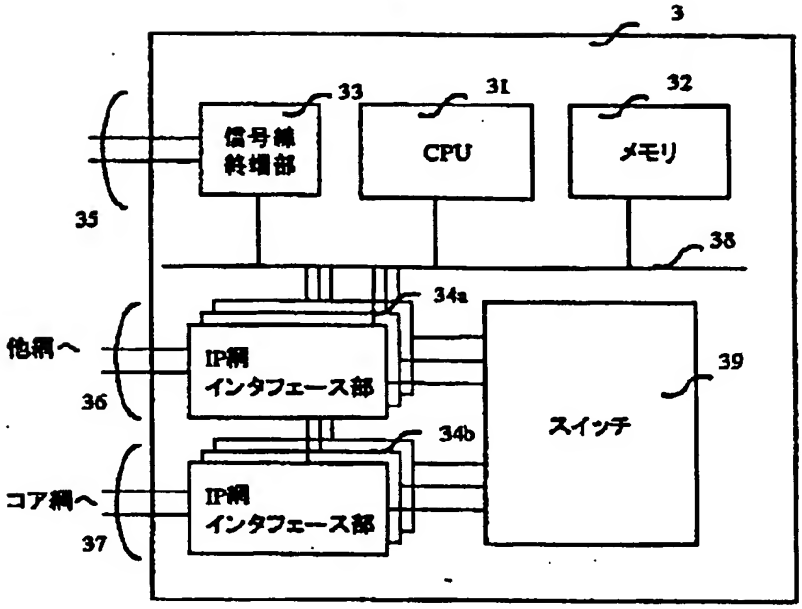
【図１】

図1



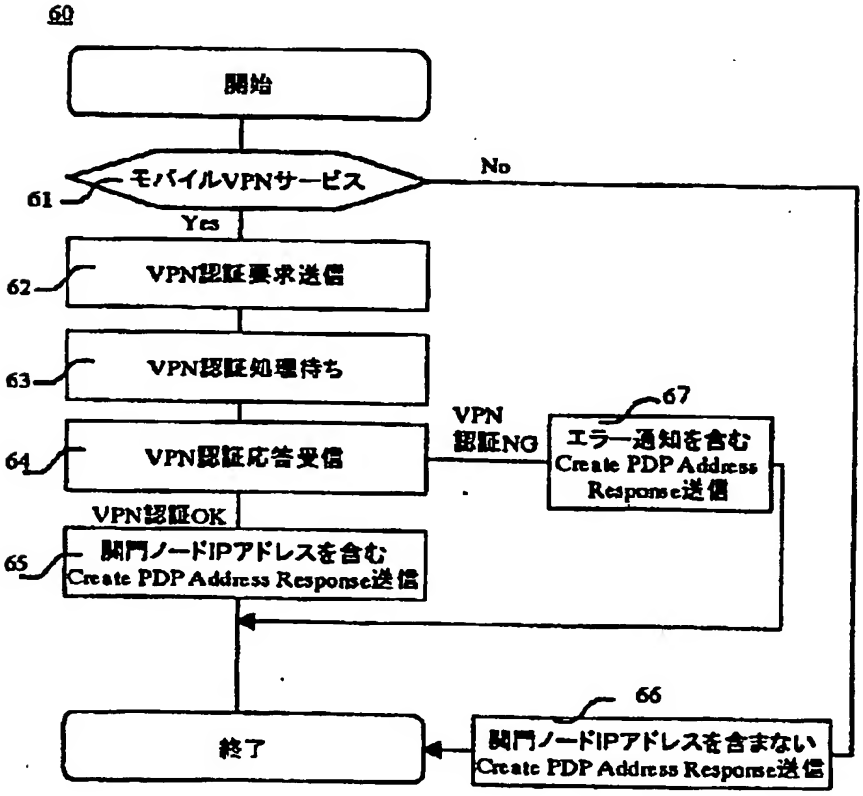
【図２】

図2


3
33
31
32
信号線
終端部
CPU
メモリ
35
38
34a
他網へ
IP網
インタフェース部
39
36
スイッチ
34b
コア網へ
IP網
インタフェース部
37

【図３】

図3


60
開始
モバイルVPNサービス
No
61
Yes
VPN認証要求送信
62
VPN認証処理待ち
63
VPN
認証NG
67
VPN認証応答受信
エラー通知を含む
Create PDP Address
Response送信
64
VPN認証OK
関門ノードIPアドレスを含む
Create PDP Address Response送信
65
66
終了
関門ノードIPアドレスを含まない
Create PDP Address Response送信

【図４】

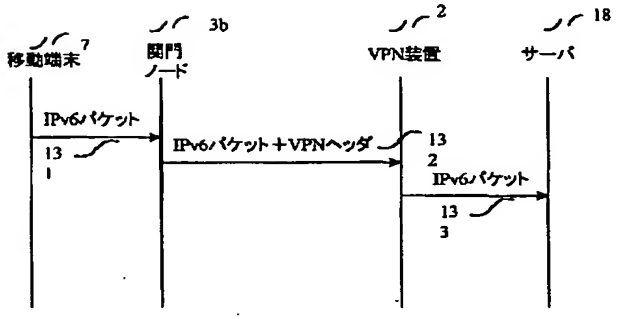
図4

300 ユーザ情報管理テーブル

301 IMSI	302 IP address	303 加入者ノード IP address	304 VPN フラグ	305 VPN トンネルID	306 VPN セッションID	
0123456789	133.144.12.34	133.150.1.2	1	xxy		300-1
0123987654	133.144.77.10	133.150.3.4	0	-		300-2
⋮	⋮	⋮	⋮	⋮		300-n

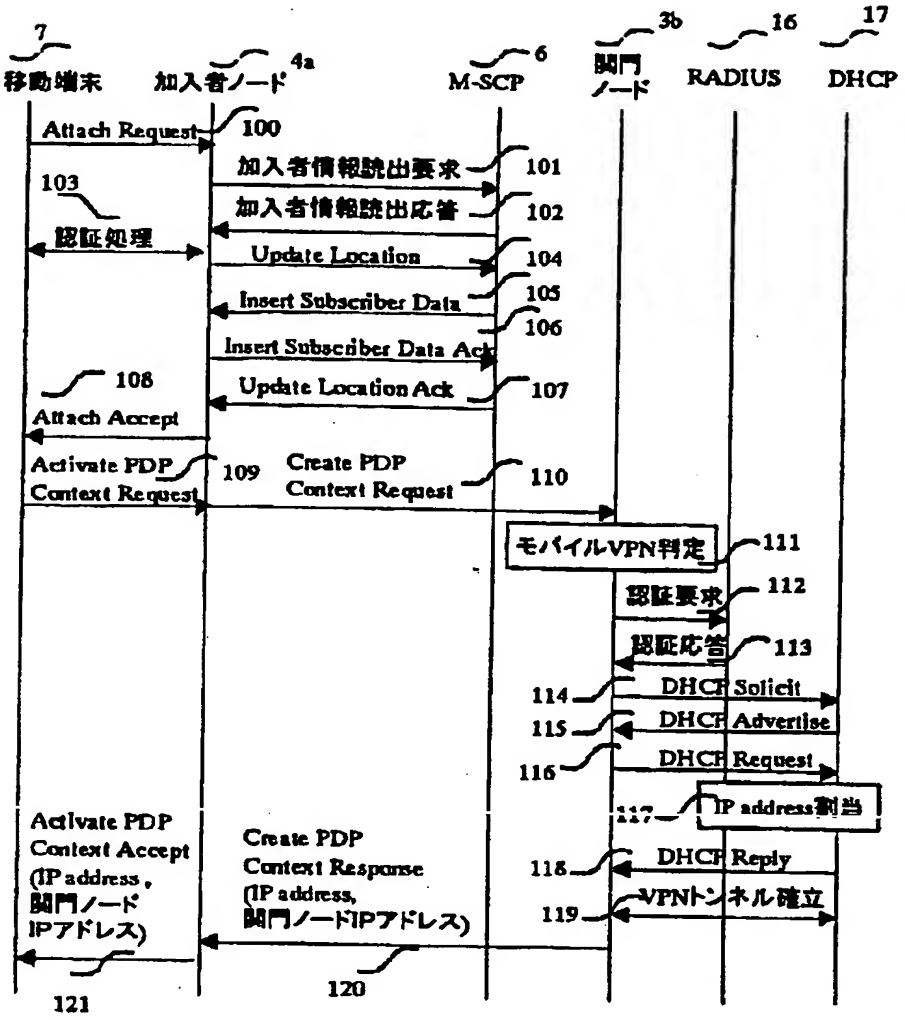
【図６】

図6



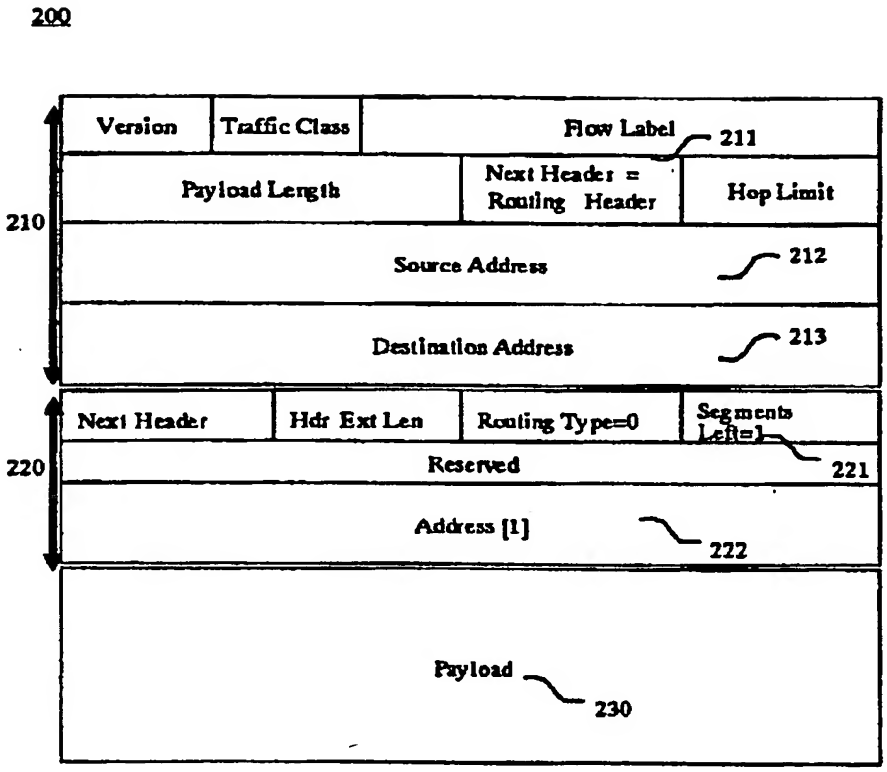
【図５】

図5


7
移動端末
加入者ノード
4a
M-SCP
6
関門ノード
3b
RADIUS
16
DHCP
17
Attach Request
100
加入者情報読出要求
101
加入者情報読出応答
102
103
認証処理
Update Location
104
Insert Subscriber Data
105
106
Insert Subscriber Data Ack
Update Location Ack
107
108
Attach Accept
Activate PDP Context Request
109
Create PDP Context Request
110
モバイルVPN判定
111
認証要求
112
認証応答
113
114
DHCP Solicit
115
DHCP Advertise
116
DHCP Request
117
IP address割当
Activate PDP Context Accept (IP address, 関門ノードIPアドレス)
Create PDP Context Response (IP address, 関門ノードIPアドレス)
118
DHCP Reply
119
VPNトンネル確立
120
121

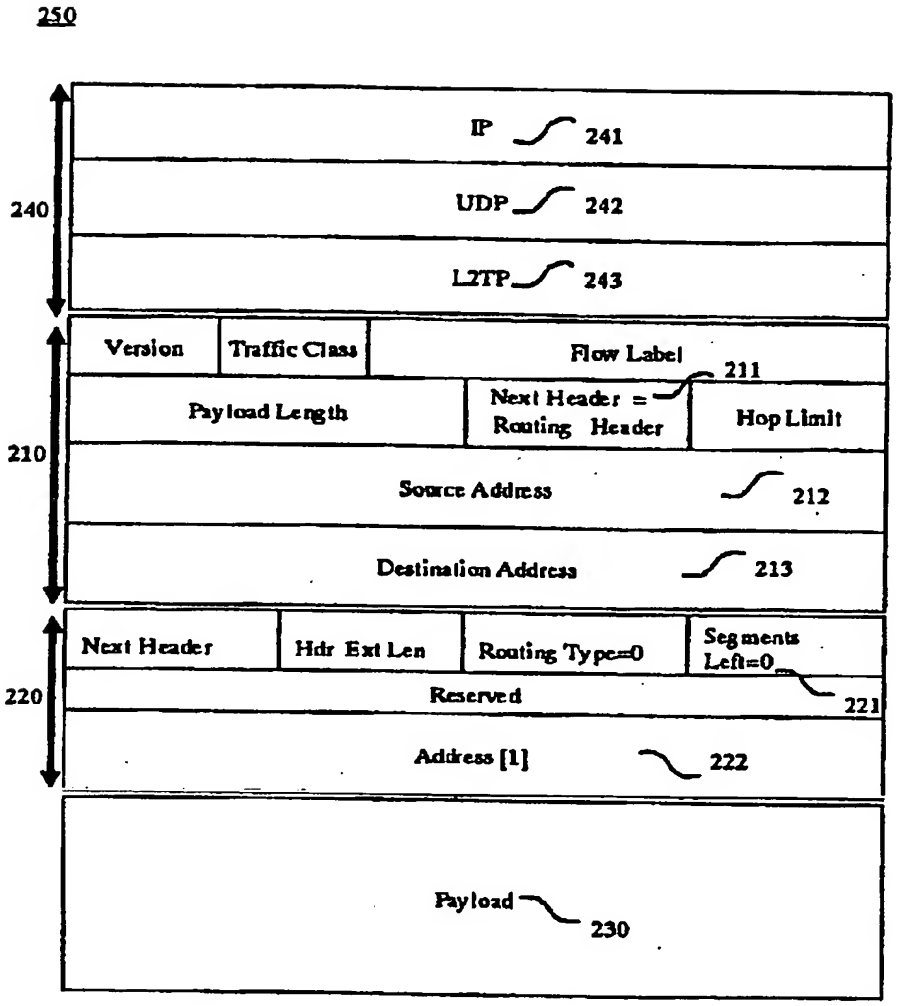
【図７】

図7


200
Version
Traffic Class
Flow Label
211
Payload Length
Next Header = Routing Header
Hop Limit
210
Source Address
212
Destination Address
213
Next Header
Hdr Ext Len
Routing Type=0
Segments Left=1
221
220
Reserved
Address [1]
222
Payload
230

【図８】

図8



フロントページの続き

(72)発明者　大石　巧
東京都国分寺市東恋ケ窪一丁目280番地
株式会社日立製作所中央研究所内
(72)発明者　柴田　治朗
神奈川県横浜市戸塚区戸塚町216番地　株式会社日立製作所ＩＰシステム事業部内

Ｆターム(参考)　5K030 GA19 HA08 HC01 HD03 HD05 HD06 JL01 JT03 LA08 LB02 LC06
5K033 AA09 CB14 CC01 DA01 DA19 EA03
5K034 AA17 BB06 DD03 EE03 FF06 HH01 HH02 LL01